EXHIBIT A

FILED
2021 NOV 12 03:55 PM
KING COUNTY
SUPERIOR COURT CLERK
E-FILED
CASE #: 21-2-15130-9 SEA

IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF KING

ALAN HALL, individually and on behalf of all others similarly situated, Plaintiffs, v. SEA MAR COMMUNITY HEALTH CENTERS, Defendant.	Cause No. **CLASS ACTION COMPLAINT**

CLASS ACTION COMPLAINT

Plaintiff Alan Hall, individually, and on behalf of all others similarly situated, brings this action against Defendant Sea Mar Community Health Centers ("SMCHC" or "Defendant"), a Washington corporation," to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. SMCHC is a health-care provider that provides medical services to patients in the State of Washington.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

2. Between the dates of December 2020 and March 2021, an unauthorized individual hacked SMCHC's IT network and obtained unauthorized access to confidential files containing current and former patients' Private Information (the "Data Breach").

3. For at least three months, the cybercriminals who hacked into SMCHC's IT network had unfettered access to files containing information pertaining to SMCHC patients (like Plaintiff).

4. Incredibly, the threat actor—known as the "Marketo gang"—stole 3 TB of sensitive data from SMCHC and thereafter posted it for sale on the "Marketo marketplace," a marketplace where the cybercriminals sell their stolen data to the highest bidder on the dark web.

5. Defendant only became aware of the hacking incident and Data Breach on June 24, 2021, when the unauthorized actor informed Defendant that it had successfully copied the sensitive data from its digital environment.

6. As a result of the Data Breach, Plaintiff and more than 650,000 Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of value of their personal information.

7. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach.

8. Information compromised in the Data Breach includes patient names, addresses, dates of birth, Social Security numbers, medical and clinical treatment information, insurance information, claims information and other protected health information as defined by the Health

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

Insurance Portability and Accountability Act of 1996 ("HIPAA") that Defendant collected and maintained (collectively the "Private Information").

9. SMCHC did not notify patients' that their Private Information was subject to unauthorized access in the Data Breach until October 2021, approximately ten (10) months after the cyberattack was launched and approximately four (4) months after the Data Breach discovered.

10. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patients' and employees' Private Information.

11. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party.

12. Defendant SMCHC maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks.

13. Upon information and belief, the mechanism of the hacking and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

14. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt notice of the Data Breach.

15. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner, as opposed to letting cyberthieves roam freely in Defendant's IT network for four (4) months.

16. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

17. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

18. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

19. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

20. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

21. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to SMCHC's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

22. Plaintiff Alan Hall is, and at all times mentioned herein was, an individual citizen of the State of Washington residing in the City of Bellingham. Plaintiff was a patient at SMCHC and received medical services and treatments from same. Plaintiff was notified of Defendant's Data Breach and his Private Information being compromised upon receiving a notice letter dated October 26, 2021.

23. Defendant SMCHC is a health-care services provider with its principal place of business at 1040 S. Henderson Street, Seattle, WA, 98108.

JURISDICTION AND VENUE

24. This Court has jurisdiction over Defendant because Defendant is organized under the laws of the State of Washington and the causes of action alleged herein arise from Defendant transacting business in Washington.

25. Venue is proper in this Court as a substantial portion of the acts and transactions that constitute violations of law complained of herein occurred in King County and Defendant

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

conducts substantial business throughout King County.

DEFENDANT'S BUSINESS

26. Defendant SMCHC is an organization that provides health, human, housing, educational and cultural services to communities in the State of Washington.

27. In the ordinary course of receiving treatment and health care services from SMCHC, patients are required to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;
- Driver's license numbers;
- Financial account information;
- Payment card information;
- Medical histories;
- Treatment information;
- Medication or prescription information;
- Beneficiary information;
- Address, phone number, and email address, and;
- Health insurance information, including health insurance plan member IDs.

28. Prior to receiving care and treatment from SMCHC, Plaintiff was required to and did in fact turn over much (if not all) of the private and confidential information listed above.

29. Additionally, SMCHC may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

30. SMCHC also creates and maintains a considerable amount of Protected Health Information (PHI) in the course of providing medical care and treatment.

31. On information and belief, SMCHC provides each of its patients with a HIPAA compliant notice of its privacy practices (the "Privacy Notice") in respect to how they handle patients' sensitive and confidential information.

32. A copy of the Privacy Notice is maintained on SMCHC's website, and may be found here: https://www.seamar.org/notice.html.

33. Due to the highly sensitive and personal nature of the information SMCHC acquires and stores with respect to its patients, SMCHC recognizes patients' Rights to Privacy in its Privacy Notice, and promises in its Privacy Notice, to, among other things, maintain the privacy of patients' protected health information.

34. SMCHC promises to maintain the confidentiality of patients' health, financial, and non-public personal information, ensure compliance with federal and state laws and regulations, and not to use or disclose patients' health information for any reasons other than those expressly listed in the Privacy Notice without written authorization.

35. As a condition or receiving medical care and treatment at Defendant's facilities, Defendant requires that each of its patients (including Plaintiff) sign a Notice of Privacy Practices Acknowledgment, which can be found here: https://www.seamar.org/seamar-downloads/covid/PatientAcknow_ENG.pdf.

36. Upon information and belief, Plaintiff did in fact sign a Notice of Privacy Practices Acknowledgment prior to receiving care or treatment from Defendant.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

37. As a condition of receiving medical care and treatment at Defendant's facilities, Defendant requires that its patients entrust it with highly sensitive personal information.

38. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

39. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

40. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE ATTACK AND DATA BREACH

41. On June 24, 2021, SMCHC was informed that certain data had been copied from its digital environment by an unauthorized actor.

42. Upon review and investigation, SMCHC determined that an unauthorized party gained access to SMCHC's IT network between the dates of December 2020 and March 2021.

43. On information and belief, and according to reports, the unauthorized actor who accessed SMCHC's IT network was the infamous Marketo gang.1 The Marketo gang is notorious for hacking businesses, exfiltrating sensitive and valuable data, and then extorting them to pay ransoms in several ways, including, but not limited to, the following:

[1] https://www.databreaches.net/wa-sea-mar-community-health-centers-discloses-breach-that-began-last-year/.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

i. Marketo has been observed sending samples of compromised data to the competitors, clients, and partners of their victims.

ii. Marketo publicly shames organizations that have not contacted the group stating the organization does not care about data security.

iii. Marketo will share subsets of data with victims as a way to prove the validity of their claims.

iv. Marketo publishes data incrementally until all information is public.[2]

44. The Marketo gang also offers up for sale the stolen data they steal on their marketplace, selling the sensitive data to the highest bidder on the Dark Web.[3]

45. Consistent with the Marketo gang's *modus operandi* of exfiltrating and stealing data, SMCHC admits that the unauthorized party "copied" the sensitive data "from its digital environment."[4]

46. Indeed, following the Data Breach, the prized data was posted on Marketo's marketplace for sale to cybercriminals, as depicted in the following image[5]:

[2] https://www.digitalshadows.com/blog-and-research/marketo-a-return-to-simple-extortion/.
[3] https://thedigitalhacker.com/irony-at-its-peak-marketo-gang-claims-to-have-bids-on-stolen-data-of-an-it-service-company-fujitsu/.
[4] https://www.prnewswire.com/news-releases/sea-mar-community-health-centers-provides-notice-of-data-security-incident-301412308.html.
[5] https://www.databreaches.net/wa-sea-mar-community-health-centers-discloses-breach-that-began-last-year/.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

47. The information stolen in the Data Breach included patient names, address, Social Security number, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment.

48. The Private Information contained in the files accessed by hackers was not encrypted.

49. Upon information and belief, the Data Breach was targeted at Defendant due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI.

50. Upon information and belief, the targeted Data Breach was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII and PHI of patients, like Plaintiff and the Class Members.

51. While SMCHC stated in notice letters sent to Plaintiff and Class Members (as well

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

as on its website) that it learned of the Ransomware Attack on June 24, 2021, SMCHC did not begin notifying impacted patients, such as Plaintiff and Class Members, until October 2021 – nearly 4 months after discovering the Data Breach.

52. Defendant SMCHC admits that its cybersecurity practices were inadequate. Indeed SMCHC admits that it is now taking the appropriate "steps to prevent a similar incident from occurring in the future," which is an implicit admission these security measures were not in place to begin with. Moreover, SMCHC stated that it "deeply regrets" that any inconvenience the Data Breach caused Plaintiff and Class Members.[6]

53. Due to Defendant's incompetent security measures, Plaintiff and the Class Members now face a present and immediate risk of fraud and identity theft and must deal with that threat forever.

54. Plaintiff believes his Private Information was stolen in the Data Breach and that said information was subsequently posted for sale on the dark web following the Data Breach, as that is the *modus operandi* of all cybercriminals, and especially the Marketo gang.

55. Defendant had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

56. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its

[6] https://www.prnewswire.com/news-releases/sea-mar-community-health-centers-provides-notice-of-data-security-incident-301412308.html.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

obligations to keep such information confidential and secure from unauthorized access.

57. Defendant's data security obligations were particularly important given the substantial increase in ransomware attacks and/or data breaches in the healthcare industry preceding the date of the breach.

58. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[7] Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[8] The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[9]

59. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

60. In 2021 alone there have been over 220 data breach incidents.[10] These

---

[7] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed June 1, 2021)
[8] *Id.*
[9] *Id* at p15.
[10] *See* Kim Delmonico, Another (!) Orthopedic Practice Reports Data Breach, Orthopedics This Week (May 24, 2021), https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

approximately 220 data breach incidents have impacted nearly 15 million individuals.[11]

61. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and ***hospitals*** are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[12]

62. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[13]

63. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

64. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

65. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

---

[11] *Id.*

[12] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited July 2, 2021).

[13] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[14] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[15]

66. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

67. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

68. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of

[14] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 15, 2021).
[15] *Id*.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

Section 5 of the FTC Act.")

69. Defendant failed to properly implement basic data security practices.

70. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

71. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

72. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

73. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

74. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

75. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

76. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Ransomware Attack.

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

77. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

78. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

79. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

80. A breach such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40

81. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S BREACH

82. Defendant breached its obligations to Plaintiff and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. SMCHC's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing or prior intrusions;

d. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

g. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

h. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

i. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

k. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

l. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

m. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

n. Failing to adhere to industry standards for cybersecurity.

83. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, and hacking attacks, SMCHC negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

84. Accordingly, as outlined below, Plaintiff and Class Members now face a present, increased, and immediate risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

85. Hacking incidents and data breaches at medical facilities like SMCHC are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

86. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[16]

87. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes,

[16] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

generally.[17]

88. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[18]

89. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names.

90. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

91. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit

[17] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[18] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[19]

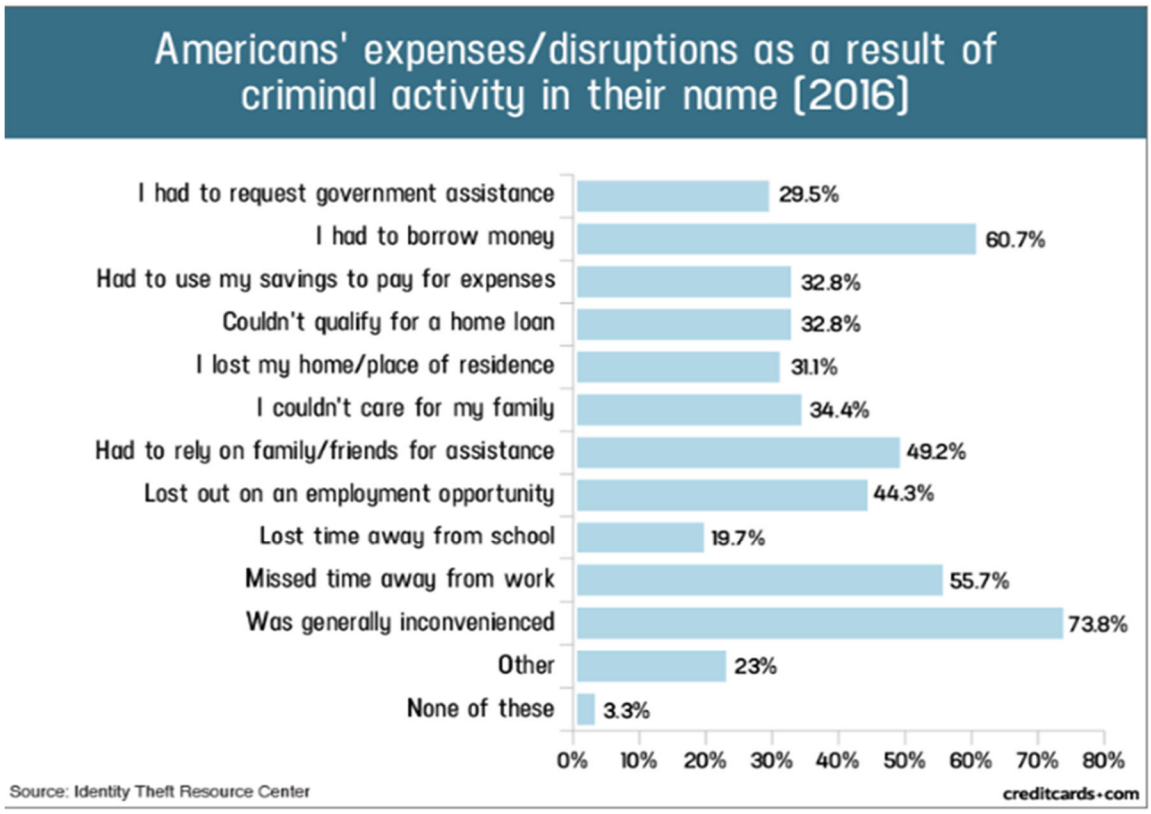
92. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

93. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

94. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[20]

[19] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Mar. 16, 2021).
[20] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711



95. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[21]

96. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider,

[21] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[22]

97. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

98. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

99. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

100. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

101. There is a strong probability that entire batches of stolen information have been

[22] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Mar. 16, 2021).

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

102. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

103. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[23] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

104. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[24] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[25] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

105. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

106. An individual cannot obtain a new Social Security number without significant

[23] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[24] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 16, 2021).
[25] *Id* at 4.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[26]

107. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[27]

108. Medical information is especially valuable to identity thieves.

109. According to account monitoring company LogDog, medical data is selling for $50 and up on the Dark Web.[28]

110. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

111. For this reason, SMCHC knew or should have known about these dangers and strengthened its network and data security systems accordingly. SMCHC was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

[26] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[27] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[28] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

Plaintiff's and Class Members' Damages

112. To date, SMCHC has done less than nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this data breach. Defendant's data breach notice letter completely downplays and disavows the theft of Plaintiff's and Class Members' Private Information, when the facts demonstrate that the Private Information was accessed and exfiltrated. The complimentary identity monitoring service offered by Defendant through Kroll is wholly inadequate as the services are only offered for 12 months and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

113. Plaintiff and Class Members have been injured and damaged by the compromise of their Private Information in the Data Breach.

114. Plaintiff's Private Information (including without limitation his date of birth, Social Security number and medical and insurance information) was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's IT network. Class Members' PII and PHI, as described above, was similarly compromised and is now in the hands of the same cyberthieves.

115. Plaintiff is a current patient of Defendant.

116. Plaintiff typically takes measures to protect his Private Information, and is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

117. Plaintiff stores any documents containing his PII and PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

118. To the best of his knowledge, Plaintiff's Private Information was never compromised in any other data breach.

119. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

120. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

121. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, and similar identity theft.

122. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

123. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

124. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by the hacker and cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

125. Plaintiff and Class Members were also damaged via benefit-of-the-bargain

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of SMCHC's computer property and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for.

126. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

127. Plaintiff and Class Members have suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

o. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;

p. Purchasing credit monitoring and identity theft prevention;

q. Placing "freezes" and "alerts" with credit reporting agencies;

r. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

s. Contacting financial institutions and closing or modifying financial accounts;

t. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

128. Moreover, Plaintiff and Class Members have an interest in ensuring that their

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing sensitive and confidential personal, health, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

129. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

130. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a present, imminent and increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

131. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

132. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

133. All individuals whose Private Information was received, gatherer, shared, obtained, or otherwise found itself in the possession of Defendant and compromised in the Data Breach.

134. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

135. Numerosity. CR 23(a)(1). The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class may approach 109,000 patients.

136. Commonality. CR 23(a)(2) & (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b) Whether Defendant knowingly concealed notification to affected customers of the Data Breach

c) Whether Defendant unreasonably delayed in notifying affected customers of the Data Breach and whether the belated notice was adequate;

d) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

e) Whether Defendant's conduct was negligent;

f) Whether Defendant violated the requirements of the Washington State Healthcare Information Act, RCW 70.02.005 *et seq*.;

g) Whether Defendant's acts, inactions, and practices complained of herein violated the Washington State Consumer Protection Act

h) Whether Defendant breached its contracts (express and implied) for data security and privacy; and

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

i) Whether Plaintiff and Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

137. Typicality. CR 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's information, like that of every other Class member, was misused, and/or disclosed by Defendant.

138. Adequacy of Representation. CR 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

139. Superiority of Class Action. CR 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all Class Members is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

140. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

141. Defendant has acted or refused to act on grounds that apply generally to the Class, as alleged above, and certification is proper under CR 23(b)(2).

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

CAUSES OF ACTION

FIRST COUNT
Violation of the Washington State Uniform Healthcare Information Act
(RCW 70.02.005 *et seq.*)
(On Behalf of Plaintiff and All Class Members)

142. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

143. Section 70.02.02 of the Revised Code of Washington provides that "Except as authorized elsewhere in this chapter, a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written authorization. A disclosure made under a patient's written authorization must conform to the authorization."

144. At all relevant times, Defendant was a health care provider because it was authorized by the laws of Washington State to provide health care in the ordinary course of their business or practice. RCW 70.02.010(19).

145. At all relevant times, Defendant collected, stored, managed, and transmitted Plaintiff and Class Members' PII/PHI.

146. Plaintiff and Class Members PII/PHI is "Health Care Information" under RCW 70.02.010(17) in that it identifies or can be readily associated with the identify of a patient and directly relates to the patient's health care or that it is a required accounting of disclosures of health care information.

147. The Revised Code of Washington requires Defendant to implement and maintain standards of confidentiality with respect to all individually identifiable PHI disclosed to them and

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

maintained by them. Specifically, RCW 70.20.020 prohibits Defendant from disclosing Plaintiff and Class Members' PHI without first obtaining their authorization to do so.

148. RCW 70.20.020-030 specifies the manner in which authorization must be obtained before PHI is released. Defendant, however, failed to obtain any authorization—let alone, proper authorization—from Plaintiff and Class Members before releasing and disclosing their PHI. As mandatorily required by RCW 70.20.150 (Security safeguards), Defendant also failed to effect reasonable safeguards for the security of all health care information they maintain, including but not limited to failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class Members' PHI. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff and Class Members' PHI was disclosed. By disclosing Plaintiff and Class Members' PHI without their written authorization. Defendant violated RCW 70.20.10 *et seq*., and its legal duty to protect the confidentiality of such information.

149. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violation of the RCW 70.20, pursuant to RCW 70.20.170, Plaintiff and Class Members also are entitled to (1) injunctive relief; (2) actual damages per Plaintiff and each Class member, and; (3) reasonable attorneys' fees and all other expenses.

SECOND COUNT
Violation of the Washington State Consumer Protection Act
(RCW 19.86.010 *et seq*.)
(On Behalf of Plaintiff and All Class Members)

150. Plaintiff repeats and re-alleges each and every factual allegation contained in all

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

previous paragraphs as if fully set forth herein.

151. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

152. Defendant is a "person" as described in RWC 19.86.010(1).

153. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

154. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

155. In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class Members' PII/PHI, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

156. Defendant also violated the CPA by failing to timely notify and concealing from

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

Plaintiff and Class Members regarding the unauthorized release and disclosure of their PII/PHI. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII/PHI, medical information, and identities.

157. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

158. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

159. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of his or her PII/PHI; (5) deprivation of the value of his or her PII/PHI, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

160. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it.

161. Plaintiff, on behalf of herself and the Class Members also seeks to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, the Plaintiff, on behalf of herself and the Class Members requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per class member.

THIRD COUNT
Negligence
(On Behalf of Plaintiff and All Class Members)

162. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

163. Plaintiff brings this claim individually and on behalf of the Class members.

164. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

165. Defendant had, and continue to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within their possession was compromised and precisely the type(s) of information that were compromised.

166. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

167. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like HIPPA and Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

168. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

169. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

170. In addition, Defendant had a duty to employ reasonable security measures under

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

171. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

172. Defendant systematically failed to provide adequate security for data in its possession.

173. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Upon information and belief, mishandling emails, so as to allow for unauthorized person(s) to access Plaintiff's and Class Members' Private Information;

b. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

c. Failing to adequately monitor the security of their networks and systems;

d. Failure to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

174. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

175. Defendant, through its actions and/or omissions, unlawfully breached their duty to

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

176. Defendant, through its actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

177. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

178. It was foreseeable that the failure to adequately safeguard Plaintiff and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

179. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

180. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding what type of Private Information has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

181. Defendant's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

182. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

183. Plaintiff seeks the award of actual damages on behalf of the Class.

184. In failing to secure Plaintiff's and Class Members' Private Information and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of herself and the Class.

185. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Defendant to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

FOURTH COUNT
Breach of Express Contract
(On Behalf of Plaintiff and All Class Members)

186. The preceding factual statements and allegations are incorporated by reference.

187. Plaintiff and Class Members entered into express contracts with Defendant that include Defendant's promise provide medical care and treatment, and the promise to protect nonpublic personal information given to Defendant or that Defendant gathers on its own from disclosure. The express contract is embodied in the Privacy Notice and the Signed Acknowledgment, and (upon information and belief) in other documents.

188. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and gave Defendant their Private Information (which also constitutes good and valuable consideration).

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

189. Defendant should have used some of Plaintiff's payments (or payments made on his behalf) to institute adequate protection of Plaintiff's Private Information, but Defendant did not.

190. As a result, Defendant exposed Plaintiff's Private Information during the Data Breach.

191. Plaintiff and Class Members thus paid Defendant for promised data security protections that they never received.

192. Had Plaintiff known of Defendant's substandard methods of protecting her Private Information, he would have sought medical care elsewhere.

193. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was accessed by unauthorized personnel as part of the Data Breach.

194. As a direct and proximate result of the breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries, and are entitled to actual, compensatory, and nominal damages.

FIFTH COUNT
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

195. The preceding factual statements and allegations are incorporated by reference.

196. Defendant provided Plaintiff and Class Members with an implied contract to protect and keep Defendant's patients' private, nonpublic personal, financial and health information when they gathered the information from each of their patients.

197. When Plaintiff and Class Members provided their Private Information to Defendant

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

198. Defendant's agreement to reasonably protect such information included compliance with healthcare industry data security standards, and with applicable data security standards that govern healthcare entities like Defendant, including HIPAA.

199. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

200. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

201. HIPAA requires covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

202. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

203. Healthcare industry standards for data security include several best practices that have been identified that a minimum should be implemented by healthcare providers like Defendant. These include, but are not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

204. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

205. Class Members who paid money to Defendant, or who had money paid on their behalf to Defendant, reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security that complied with healthcare industry data security standards and applicable regulations like HIPAA. Defendant failed to do so.

206. Plaintiff and Class Members would not have provided their personal, financial or health information to Defendant, but for Defendant's implied promises to safeguard and protect Defendant's patients' private personal, financial, and health information.

207. Plaintiff and Class Members performed their obligations under the implied contract when they provided their private personal, financial, and health information as a patient and when they paid for the services provided by Defendant.

208. Defendant breached the implied contracts with Plaintiff and Class Members by failing to protect and keep private the nonpublic personal, financial, and health information provided to them about Plaintiff and Class Members.

209. As a direct and proximate result of Defendant's breach of their implied contracts, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

SIXTH COUNT
Breach of Confidence
(On Behalf of Plaintiff and All Class Members)

210. The preceding factual statements and allegations are incorporated by reference.

211. At all times during Plaintiff's and the Class's interactions with Defendant, Defendant were fully aware of the confidential and sensitive nature of Plaintiff's and the Class's PII and PHI that Plaintiffs and the Class provided to Defendant.

212. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class's PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

213. Plaintiff and the Class provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

214. Plaintiff and the Class also provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII and PHI from unauthorized disclosure.

215. Defendant voluntarily received in confidence Plaintiff's and the Class's PII and PHI with the understanding that PII and PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

216. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Class's PII and PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class's confidence, and without their express permission.

217. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

and the Class have suffered damages.

218. But for Defendant's disclosure of Plaintiff's and the Class's PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and the Class's PII and PHI as well as the resulting damages.

219. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class's PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class's PII and PHI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class's PII and PHI.

220. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

fails to undertake appropriate and adequate measures to protect the PII and PHI of current and former patients and their beneficiaries and dependents; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

221. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

FRANK FREED
SUBIT & THOMAS LLP
Suite 1200 Hoge Building, 705 Second Avenue
Seattle, Washington 98104-1798 ~ (206) 682-6711

E. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

F. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class Members;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

RESPECTFULLY SUBMITTED this 11th day of November, 2020.

FRANK FREED SUBIT & THOMAS LLP

By: */s/ Michael C. Subit*

Michael C. Subit, WSBA No. 29189
705 Second Avenue, Suite 1200
Seattle, Washington 98104-1798
(206) 682-6711 (phone)
(206) 682-0401 (fax)
msubit@frankfreed.com

(Local Counsel)

MASON LIETZ & KLINGER LLP

Gary E. Mason (*pro hac vice forthcoming*)
David K. Lietz (*pro hac vice forthcoming*)
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Phone: 202.640.1160
gmason@masonllp.com
dlietz@masonllp.com

MASON LIETZ & KLINGER LLP

Gary M. Klinger (*pro hac vice forthcoming*)
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (312) 283-3814
Fax: (773) 496-8617
gklinger@masonllp.com

(Lead Counsel)

Attorneys for Plaintiff and the Proposed Classes